| | | | |
|---|---|---|---|
| ***Supplemental Notice of Allowability*** | **Application No.**<br>09/502,478 | **Applicant(s)**<br>ATTWOOD ET AL. | |
| | **Examiner**<br>Thomas M. Ho | **Art Unit**<br>2134 | |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--***

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *11/18/05*.

2. ☒ The allowed claim(s) is/are *1-16*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

**Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 3/13/00
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (~~PTO-413)~~, Paper No./Mail Date ~~12/22/05, 2/17/05~~. 6/26/06
7. ☒ Examiner's Amendment/~~Comment~~
8. □ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

## EXAMINER'S AMENDMENT

**1.** An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

~~Authorization for this examiner's amendment was given in a telephone interview with Steven Greenberg on 2/17/06.~~

Authorization for a supplemental examiner's amendment was given in a telephone interview with Scott D. Paul on 6/26/06.

~~*Amendment of Claims*~~

~~1. A method of preventing a flooding attack on a network server in which a large number of requests are received for connection to a particular port number on the server, comprising:~~

~~recognizing a particular host connecting to the port number on the server;~~

~~calculating a number of connections to the port attributed to the host;~~

~~determining, in response to a request from the host for a connection to the port, if the number of connections to the port attributed to the host exceeds a prescribed threshold, and, if so, denying the request for a connection.~~

~~5. Apparatus for preventing a flooding attack on a network server in which a large~~ number of requests are received for connection to a particular port number on the server, comprising:

means for recognizing a particular host connecting to the port number on the server;

means for calculating a number of connections to the port attributed to the host;

means for determining, in response to a request from the host for a connection to the port, if the number of connections to the port attributed to the host exceeds a prescribed threshold, and

means responsive to the determining means for denying the request for a connection.

9. A storage media containing program code segments for preventing a flooding attack on a network server in which a large number of requests are received for connection to a particular port number on the server, comprising:

a first code segment activated to recognize a particular host connecting to the port number on the server;

a second code segment to calculate a number of connections to the port attributed to the host;

a third code segment activated in response to a request from the host for a connection to the port for determining if the number of connections to the port attributed to the host exceeds a prescribed threshold, and

a fourth code segment responsive to the third code segment for denying the request for a ~~connection.~~

10. The media of claim 9 in which the second code segment ~~further comprises:~~

a fifth code segment for overriding the denial and allowing the request if a quality of service parameter pertaining to the requesting host permits the override.

11. The media of claim 10 further comprising a sixth code segment for denying a connection request in any event if the number of available connections to the port are less than a constrained threshold.

12. The media of claim 9 or claim 10 or claim 11 further comprising:

a seventh code segment for calculating the prescribed threshold by multiplying a percentage P by the number of available connections remaining for the port.

13. A carrier wave containing program code segments for preventing a flooding attack on a network server in which a large number of requests are received for connection to a port number on the server, comprising:

a first code segment activated to recognize a particular host connecting to the port number on the server;

a second code segment to calculate a number of connections to the port attributed to the host;

~~a third code segment~~ activated in response to a request from ~~the host for a connection to~~ the port for determining if the number of connections to the port attributed to the host exceeds a prescribed threshold, and

a fourth code segment responsive to the third code segment for denying the request for a connection.

14. The carrier wave of claim 13 in which the second code segment further comprises:

a fifth code segment for overriding the denial and allowing the request if a quality of service parameter pertaining to the requesting host permits the override.

15. The carrier wave of claim 14 further comprising a sixth code segment for denying a connection request in any event if the number of available connections to the port are less than a constrained threshold.

16. The carrier wave of claim 13 or claim 14 or claim 15 further comprising:

a seventh code segment for calculating the prescribed threshold by multiplying a ~~percentage P by~~ the number of available connections ~~remaining for the port.~~

*Amendment of Specification*

On page 4 of the specification on the last paragraph, please omit the sentence

*"This is the subject matter of patent application number ____."*

The last paragraph of page 4 should be amended as follows:

A similar technique can be applied to connectionless traffic, such as UDP datagrams. ~~This is the subject matter of patent application number~~ ____.

### *Reasons for Allowance*

The claims are still allowable for the same reasons as set forth in in the notice of allowance mailed on

~~2. Applicant's independent claims recite the limitation,~~

- "Recognizing a particular host connecting to the port number on the server"

Previously, the Examiner rejected the independent claims using Schuba, US patent, 6725378.

Schuba (Column 4, lines 53-67) detects if a particular maximum number of connections have been reached per port. If it is determined that the maximum number of connections on that port has been reached, Schuba will discard all further connections per port.

Schuba however fails to disclose a particular recognition of the connections coming about from a ~~singular host. Instead, Schuba performs a blanket operation where all further connections to the~~

~~port are sealed off, rather than denying the request for a~~ connection to the port from an attributed and "recognized" host.

A rejection based on Pars Mutaf "Defending against a Denial of Service Attack on TCP" was also previously made.

Mutaf, page 6, discloses a detection of an attack where if the number of received SYN segments per second by a given TCP port exceeds a maximum or prescribed threshold, the network monitor is to consider the event an attack.

Mutaf additionally fails to recite an explicit "recognition" of the attack arising from an identified host, and only identifies the attack based on the threshold of the port, rather than the two aspect analysis of recognizing the host and determining if the number of connections exceeds a threshold.

Mutaf and Schuba have been identified as the Examiner as the closest art of record, both of them deficient on the limitation of "Recognizing a particular host connecting to the port number on the server". Indeed, the fact that Schuba and Mutaf suffer from the same deficiency appears to speak of a en explicit and reasonably well identified boundary on the current state of the art regarding "Denial of Service" identification and flooding attack protection.

For this reason, ~~the Examiner~~ has withdrawn all rejections, and has allowed the pending claims.

***Conclusion***

**3.** Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,
Jacques Louis-Jacques 571-272-6962
~~Gregory A. Morse~~ can be reached on ~~(703)308-4789~~. The fax phone numbers for the organization where this application or proceeding is assigned are ~~(703)746-7239 f~~or regular communications and ~~(703)746-7238 f~~or After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is ~~(703)306-5484.~~

TMH Thomas M Ho

February 18th, 2006